



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/665,338

09/17/2003

Yosef Stein

AD-356J

7044

7590  
Iandiorio & Teska  
260 Bear Hill Road  
Waltham, MA 02451-1018

01/11/2007

EXAMINER

ZAND, KAMBIZ

ART UNIT

PAPER NUMBER

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
--	-----------	---------------

3 MONTHS

01/11/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/665,338	<b>Applicant(s)</b> STEIN ET AL.	
	<b>Examiner</b> Kambiz Zand	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 17 September 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 12-14 and 29 is/are rejected.
- 7) ☒ Claim(s) 2-11, 16-28, 30 and 31 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.


#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
KAMBIZ ZAND  
PRIMARY EXAMINER

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>09/03 and 02/2006</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. **Claims 1-31** have been examined.

#### ***Information Disclosure Statement PTO-1449***

2. The Information Disclosure Statement submitted by applicant on 09/17/2003 & 02/23/2006 has been considered. Please see attached PTO-1449.

#### ***Claim Objections***

3. **Claims 2 AND 18** are objected to because of the following informalities: typo error. Examiner suggests the following corrections:

##### **Claims 2 and 18:**

4. Replacement of "m-1" (line 2) with "m-1" (remove the underlining).
5. Please check for all similar typo error.

#### ***Claim Rejections - 35 USC § 101***

6. 35 U.S.C. 101 reads as follows:
  - a. Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.
7. **Claims 1-31** are rejected under 35 U.S.C. 101 because it has no tangible result. Claim 1 does not disclose any tangible result or it is not clear what the tangible result is. Also claim 1 only disclose an encryption engine which could be software only which

Art Unit: 2132

creates ambiguity if applicants software have a tangible embodiment since the software is not stored on any tangible medium.

Examiner suggests introduction of "storing" on a tangible medium and amendments that clearly shows the tangible result into independent claim 1. if such tangible result exists in claim 1 already please refer to it in the response to this office action.

### ***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1, 12-15 and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by McCanny et al. (2003/0039355 A1) cited in the IDS by Applicant.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

**As per claim 1** McCanny et al. (2003/0039355 A1) disclose an advanced encryption standard (AES) engine with real time S-box generation comprising: a Galois field

Art Unit: 2132

multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in  $GF^1(2^m)$  and applying an affine over  $GF(2)$  transformation to obtain a subbyte transformation (**see fig.1a-c,3,5 and associated texts including item 32 of fig.3 and 54 of fig.5**); and a shift register system for transforming said subbyte transformation to obtain a shift row transformation (**see fig.2, item 32;fig.5, item 54 and associated texts**); said Galois field multiplier system being responsive in a second mode to said shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of said first data block (**see fig.4,5,5a,11 and associated texts in full**). **Also see [0040-0062 and all other related paragraph.**

**As per claim 12** McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes at least one Galois field linear transformer and an associated polynomial multiplier (**see fig.5 and associated texts;[0048-54]**..

**As per claim 13** McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 in which said Galois field multiplier system includes a reconfigurable matrix of cells (**see fig.7 and associated texts**).

**As per claim 14** McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a key generator for providing a plurality of round keys (**see fig.4 and associated text including round 0 to round final**).

**As per claim 14** McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 14 in which said key generator includes a key generator circuit responsive to a master key to generate said round keys (**see fig.3-5 and associated text**).

**As per claim 29** McCanny et al. (2003/0039355 A1) disclose the advanced encryption standard (AES) engine with real time S-box generation of claim 1 further including a plurality of Galois field multiplier systems for simultaneously processing a plurality of subbytes (**see fig.5 and associated text including item 54-58 where it disclose multiple subbytes**).

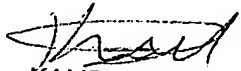
***Allowable Subject Matter***

10. **Claims 2-11, 16-28, 30 and 31** would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 101, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

### Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: please see enclosed PTO-892.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally be reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned are (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
KAMBIZ ZAND  
PRIMARY EXAMINER

01/05/2007

AU 2132